

27th February 2026

Dear [REDACTED]

Thank you for your request of 12th February 2026 in which you asked about software-based data erasure of end-of-life IT equipment. The Royal Parks response is as follows:

Under the Freedom of Information Act 2000, please provide the following recorded information held by your department regarding assurance processes for software based data erasure of end of life IT equipment. For clarity, this request relates solely to software based data destruction. Please exclude physical destruction methods such as shredding, crushing, degaussing or disintegration.

- 1. Please confirm whether departmental policy, contractual terms or internal procedures require an explicit outcome based warranty or guarantee confirming that personal data has been rendered irretrievable through software based erasure, whether carried out internally or by an external provider.**

The Royal Parks does not hold any recorded policy, internal procedure, or contract clause that requires an explicit outcome-based warranty or guarantee for software-based data erasure, whether performed internally or by an external provider.

- 2. Where software based data destruction is performed internally, what recorded evidential assurance does the department rely upon to conclude that the final data state is irretrievable?**

The Royal Parks does not hold any recorded internal procedure for performing software-based data erasure.

The organisation relies on external certified data-sanitisation services rather than carrying out software erasure internally.

- 3. Where software based data destruction is performed by a third party provider, does the department hold recorded information demonstrating that any warranty or assurance provided explicitly extends to the software erasure method used and its claimed effectiveness? If so, please confirm the recorded nature of that verification.**

Recorded information confirms that The Royal Parks uses OCM Business Systems for IT asset disposal.

OCM performs software-based sanitisation using Blancco, which is certified by the UK National Cyber Security Centre (NCSC).

The Royal Parks holds provider-supplied documentation such as data-sanitisation confirmations, asset registers, compliance paperwork, and certification evidence (e.g. ISO standards, ICO registration, WEEE compliance).

No recorded information is held showing that OCM provides an explicit outcome-based warranty for data irretrievability.

4. Where no explicit outcome based warranty is required or provided, what recorded form of evidential assurance does the department rely upon to conclude that software based erasure has rendered personal data irretrievable?

Where no explicit guarantee is held, The Royal Parks relies on the documentation provided by the asset disposal provider, including confirmation of sanitisation, asset-level reports, and certification records.

No further outcome-based or independently verified evidence is held.

I am not requesting technical configuration detail, security sensitive information or supplier specific vulnerabilities. I am seeking confirmation of the assurance model relied upon for software based data destruction.

I hope this information satisfies your request.

Right of Review

If you are dissatisfied with this response, you may request an internal review within 40 working days of the date of this letter, quoting the reference at the top of the page and should be addressed to:

Records Manager
The Royal Parks
The Old Police House
Hyde Park
London
W2 2UH

Email: records@royalparks.org.uk

If you are not content with the outcome of the internal review, you have the right to apply directly to the Information Commissioner for a decision, quoting the reference at the top of the page. The Information Commissioner can be contacted at:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Yours sincerely,

Records Manager | records@royalparks.org.uk | www.royalparks.org.uk |
The Old Police House | Hyde Park | London | W2 2UH